Amendments to the Drawings:

The attached drawings sheet is a new drawing sheet. The attached drawings sheet illustrates an exemplary hardware embodiment of the invention. The drawing is supported by, at least, the original disclosure of the invention on page 1, lines 2-5, and in the claims as originally filed.

Attachment: New drawing sheet including Figure 5.

Remarks:

This paper is in response to the office action dated September 28, 2005 with respect to Application No. 09/646,640. Claims 10-15 stand rejected. Applicant cancels claim 13, amends Claims 10, 11, 12 and 14, and adds new Claims 16 and 17. Claims 10-12, and 14-17 are pending in the Application.

Applicant acknowledges with thanks the Examiner's indication that the new drawings, received on August 18, 2005, are acceptable.

Applicant has added a new Figure 5 and corresponding description for the specification. The support for these amendments may be found in the originally filed application, for example, in page 1, lines 2-5, page 1, line 26, page 6, lines 7-8, and the originally filed claims.

Claim objections

Claim 13 stands objected to as not further limiting the parent claim from which it depends. Claim 13 has been cancelled herein. Therefore, applicant respectfully submits that the objection is moot and should be withdrawn.

Claim Rejection under 35 USC 112, second paragraph

Claims 11 and 12 stand rejected under 35 U.S.C. 112, second paragraph as being indefinite for failing to particularly and distinctly claim the subject matter of the invention. Claims 11 and 12 have been amended. Applicant respectfully submits that all limitations of Claims 11 and 12 have, where required, proper antecedent basis in the claim or the claim from which they depend. Furthermore, the limitations of Claims 11 and 12 are supported by the specification, for example, at least on page 5,

lines 5-7, and on page 5, lines 16-19. Accordingly, Claims 11 and 12 meet the requirements of both the first and second paragraph of 35 USC 112.

Claim Rejection under 35 USC 101

Claims 10-15 were rejected under 35 USC 101 as directed to non-statutory subject matter as not being tangible. Claim 10 has been amended to recite hardware aspects of the method of the invention, particularly, that the method is directed to "causing the microprocessor to randomly modifying the order of execution of operations involving manipulations of data elements contained in the memory from one cycle to another ..." (Claim 10). Thus, Claim 10 is directed to the operation of a microprocessor. Accordingly, Claim 10 as amended recites patentable subject matter. Applicant therefore respectfully requests withdrawal of the rejection.

Claim Rejection under 35 USC 103(a)

Claims 10-15 stand rejected under 35 U.S.C. 103(a) as being unpatentable over FIPS PUB 46-2 "Data Encryption Standard" (hereinafter FIPS 46-2) in view Collberg et al. "A Taxonomy of Obfuscating Transformations" (hereinafter Collberg).

Applicant traverses the rejections applicable to the remaining claims and respectfully requests withdrawal of any rejection and an indication of allowance for the reasons set forth below.

As described in the specification, the claims are directed to solving a current problem in the state of the art concerning measurement of power consumption of an electronic device (by means of an oscilloscope) and observing its behavior. For example, a power trace of the device that performs an encryption using the DES algorithm. The power consumption is not constant and reveals some patterns. Knowing that DES takes

typically 16 rounds to encrypt the input data it is possible to identify the rounds in the 16 repeating patterns in the power trace. Although this is an interesting observation it does not give an answer to the more important question: what is the key used for this encryption? Hackers proposed Differential Power Analysis (DPA) to retrieve the key of a cryptographic algorithm by analyzing several of measured power traces. An attacker only needs to know either the clear text (input) or cipher test (output) of the algorithm. The basic idea behind the attack is the assumption that there is a correlation between data values being processed by the device and the power consumption. In other words and for explanation purposes: it is conceptually assumed that processing a bit value zero uses less energy than processing a bit value one (or vice versa).

By using different input values it results in a small difference in power consumption and a key can be identified by inspection of differential traces. By computing differential traces it is possible to "identify" the clock cycles where input data is being processed. Moreover, by considering all input bits to a cryptographic algorithm and creation of differential traces for each pair (a trace for a bit value zero and a trace for a bit value one), it is possible to identify the exact timing of their appearance in the program code. In situations where noise prevents the recognition of peaks in the differential trace it is possible to increase the number of samples and compute a differential trace out of many individual traces.

The Examiner has failed to establish a *prima facie* case of obviousness. "To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to

combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations." MPEP 2143. The Examiner has failed to meet this burden, at least with respect to the final criteria (Applicant reserves the right to argue the first and second criteria in a future office action response or on appeal).

Claim 10 recites, for example, the limitations of "operating the microprocessor to randomly modifying the order of execution of operations involving manipulations of data elements contained in the memory from one cycle to another, a cycle being a complete execution cycle of the algorithm or an intermediate cycle of a group of operations, said operations being operations whose order of execution relative to the others does not affect the result" making the differential analysis between races is made difficult or even impossible because processing orders are modified.

Neither FIPS 46-2 nor Collberg, alone or in combination, teach the elements of Claim 10 and, specifically protecting data elements from discovery by analysis of a microprocessor's electric power consumption by "randomly modifying the order of execution of operations involving manipulations of data elements contained in the memory from one cycle to another" (Claim 10).

The Examiner has acknowledged that "FIPS 46-2 does not disclose randomly modifying the order of execution of operations from one cycle to another, a cycle being a complete execution cycle of the algorithm or an intermediate cycle of a group of operations, the operations being the operations whose order of execution relative to the others does not affect the result" (Office Action, paragraph spanning pages 4 and 5).

Collberg also fails to teach or suggest that limitation.

Collberg describes obfuscation methods. Such methods are intended to limit the risks that a malicious person "reconstitutes" by reverse-engineering the algorithmic structure of a software program from the low-level language (e.g., machine-readable language). This risk is increased with the use of Java language. See, for example, Page 1, Introduction: "Given enough time, effort and determination, a competent programmer will always be able to reverse engineer any application."

Collberg's objective is to propose methods to make very difficult or impossible:

- the reconstitution
- from a low level language software program,
- of the associated algorithmic structure of this software program.

The present invention proposes methods for operating a microprocessor of a chip card to make very difficult or impossible

- the reconstitution
- from external monitoring of the **microprocessor's electric power consumption.**
- of data elements stored in the memory of a chip card.

Thus, the objective of Collberg is very different from the solutions achieved by the present invention. It is therefore not surprising that the solution proposed by Collberg is very different from the one presented in the claimed invention of the present application.

Collberg fails to disclose, for example, to "randomly modifying the order of execution of operations from one cycle to another" as claimed in Claim 10. In fact, Collberg only proposes to randomize the placement of any item in the source application. The implication of that would be, for

example, in a group of N successive statements, the statement locations in the group are positioned randomly. Consider:

A = A + i

B = B + 2i

C = A + B

a resultant randomization could be:

B = B + 2i

A = A + i

C = A + B

thus, modifying the ordering of the statement.

However, note that according to Collberg, whatever randomization process that is used, the target program that is obtained (from the source program) remains static and the execution order thus obtained is not modified during execution. Thus, Collberg does not teach or suggest a "random modification of the order of execution from one cycle to the other" as claimed in Claim 10.

In particular, the Examiner refers to "loop unrolling" discussed in Collberg. The transformation made from a source program loop to target a program loop is shown in Page 17, Figure 17 (b). Unrolling loop solution consists in transforming a loop as follows :

```
for (i = 2, I < (n-1), i++)
     a[i] += a[i-1]*a[i+1]
To a target  loop as follows :
for (i=2,i<(n-2_,i+=2) {
     a[i] += a[i-1]*a[i+1];
     a[i+1] += a[i]*a[i+2];
};
if (((n-2) % 2) == 1)
     a[n-1] += a[n-2]*a[n]
```

It is clear from the disclosure in Collberg that with respect to the target loop thus obtained, there is no modification of the order of execution of operations from one cycle to another. The successive operations of the loop will always be executed in the same order.

In addition the Examiner uses the teaching of Section 6.3.4 related to the Loop transformation and Section 6.4 related to the ordering transformations.

While Section 6.3.4 proposes obfuscation methods based upon a complexification of a program loop, clearly Section 6.3.4 does not propose "randomly modifying the order of execution of operations from one cycle of the loop to another".

Section 6.4 proposes to randomize the placement of items in a program for obfuscation purposes but does not describe or suggest that this randomization applies to the "order of execution of operations from one cycle to another", as claimed in Claim 10. It appears from the reading of Section 6.4 that this randomization of items applies only one time for producing the target program from the source program and not recurrently thereby randomly modifying the order of execution of operations from one cycle to another.

Considering that "randomly modifying the order of execution of operations from one cycle of the loop to another" is lacking from both

Collberg and FIPS 46-2, at least one further modification would be required to the references or to the combination in order to construct applicant's claimed invention therefrom. However, a person of ordinary skill in the art would not be motivated to modify Collberg to include the step of "randomly modifying the order of execution of operations from one cycle of the loop to another". "First, there must be some suggestion or motivation ... to modify *the reference"* MPEP 2143. That motivation may come from the reference itself or knowledge generally available to one of ordinary skill in the art. MPEP 2143. Collberg does not provide that motivation, nor would it be part of the knowledge generally available to one of ordinary skill in the art.

"If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." MPEP 2143.01 *quoting* In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious" MPEP 2143, *quoting,* In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). It should be noted that the present invention deals with randomization during the execution of the cryptographic operations. As discussed herein above, Collberg teaches the obfuscation of source code for the purpose of making the structure of the source code less understandable by a programmer trying to reconstitute the operation of a program. A programmer seeking to reverse-engineer a program would not be examining the program code during the execution of the program, but rather as a static file created by the obfuscator. In fact, Applicants respectfully request the Examiner take judicial notice of that typically programs do not change during execution and if there is a change in a program at all during execution, that change is not to the underlying

source code that a programmer may wish to reverse engineer. Therefore, to make a modification to Collberg to include "randomly modifying the order of execution of operations from one cycle of the loop to another" (Claim 10), would, indeed, change the principle of operation of Collberg and make Collberg unsuitable for its intended purpose. Accordingly, Applicants respectfully submit that there would be no motivation for making the necessary modification to Collberg.

For the reasons provided above, a prima facie case for obviousness has not been established for Claim 10 based on the FIPS 46-2 or Collberg references, taken alone or in combination.

A prima facie case of obviousness has also not been established with respect to Claim 14. Claim 14 recites "operating the microprocessor to determine a processing order of the bits for the execution of the permutation step". Neither FIPS 46-2 nor Collberg teach or suggest such an element.

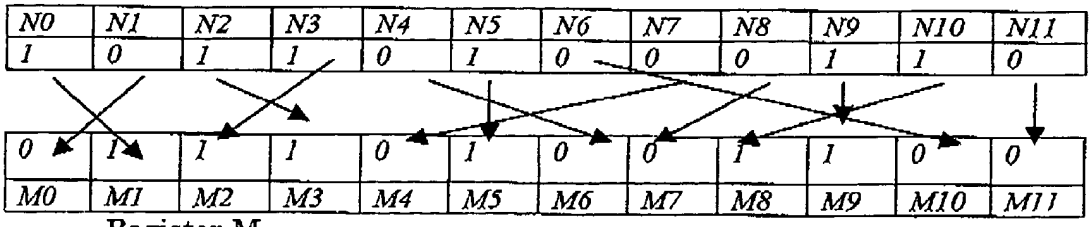
The Examiner has acknowledged that "FIPS 46-2 does not disclose a random determination of a processing order of the bits for the execution of the permutation step" (Office Action, page 6, numbered paragraph 21).

Collberg also fails to teach or suggest "operating the microprocessor to determine a processing order of the bits for the execution of the permutation step" (Claim 14). Claim 14 proposes a method for operating a microprocessor to protect a key contained in a memory of a chip card from discovery by analysis of the microprocessor's electric power consumption, the method using a symmetric cryptographic algorithm of the DES-type with a permutation step and wherein the method comprises the random determination of the processing order of the bits for the execution of the permutation step.

In DES, a permutation step is one among several steps that can include substitution, multiplication, etc.

An example permutation is illustrated below :

Register N



Register M

Such a permutation requires that each one of N successive bits be permutated from rank n to rank m. For example in the above drawing, the operations are made as follows :

Step 1- Firstly the content of register bit N0 is written in register bit M1, then

Step 2- the content of register bit N1 is written in register bit M0, then

Step 3 - the content of register bit N2 is written in register bit M3, then

Step 4 - the content of register bit N3 is written in register bit M2, then

Step 5 - the content of register bit N4 is written in register bit M6, then

Step 6 - the content of register bit N5 is written in register bit M5, then

Step 7 - the content of register bit N6 is written in register bit M10, then

Step 8 - the content of register bit N7 is written in register bit M4, then

Step 9 - he content of register bit N8 is written in register bit M7, then

Step 10 - the content of register bit N9 is written in register bit M9, then

Step 11 - the content of register bit N10 is written in register bit M8, and then

Step 12 - the content of register bit N11 is written in register bit M11.

The invention proposes to randomize the order of the operations Step 1 to Step12, by making random the order of these operations. As a result, the first bit to be permuted is not necessary the first bit of the "input data" but a bit selected randomly within the "input data", the second bit to be permuted is not necessarily the second bit of the "input

data" but a bit selected randomly within the input data, and similarly for the other bits.

It should be noted that the permutation result is not modified but the processing order according to which the bits are permuted is determined randomly.

In making the obviousness rejection of Claim 14, the Examiner particularly refers to Section 6.4 of Collberg. As discussed herein above, according to Collberg, whatever be the randomization process that is used, the target program that is obtained (from the source program) remains always the same thereafter and the execution order thus obtained is not modified thereafter. Therefore, it must be concluded that Collberg does not propose or suggest to operate a microprocessor to "randomly determine the processing order of the bits for the execution of the permutation step".

It is also noted that the Examiner argues that the steps (permutation, key permutation, s-box substitution, p-box substitution, ...) in each round are commutative thereby rendering our invention obvious in view of Collberg. Claim 14 is not based upon the use the commutative property of different major steps (substitution, permutation, etc.) in DES. In fact, it is proposed in Claim 14 to randomize the processing order of the bits, which randomization affects only the permutation operation order, and not the relative order of the different DES steps such as permutation, substitution, etc.

As with Claim 10, discussed hereinabove, because both FIPS 46-2 and Collberg fail to teach or suggest "operating the microprocessor to determine a processing order of the bits for the execution of the permutation step" (Claim 14), a further modification of either reference or the combination would be required to achieve applicant's claimed invention. As with Claim 10, such a modification is not suggested by these references. Collberg's obfuscator would not benefit from a permutation of the steps performed because the purpose of the obfuscator is to obfuscate

the source code of a program and not the operation of the program during execution. That modification would both render Collberg unsuitable for its intended purpose and radically change the operation of Collberg. Therefore, the person of ordinary skill in the art would not be motivated to make such a modification.

For the reasons provided above, a *prima facie* case for obviousness has not been established based on the FIPS 46-2 or Collberg references, taken alone or in combination.

Claims 11, 12, 15, 16, and 17 depend from Claims 10 and 14, respectively, provide further unique and non-obvious combinations, and are patentable, at least, for the reasons given in support of Claims 10 and 14 and by virtue of such further combinations.

The Examiner has filed to establish a *prima facie* case of obviousness. "If examination at the initial stage does not produce a prima facie case of unpatentability, then without more the applicant is entitled to grant of the patent." In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992), *quoted in* In re Lowry, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994). Thus, for the reasons given above, Applicants respectfully request withdrawal of the rejection of the Claims and their early allowance.

CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request consideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Applicants respectfully request that a timely Notice of Allowance be issued in this application.

Respectfully submitted,

Date: December 28, 2005

Pehr Jansson
Registration No. 35,759

Attn: Pehr Jansson
Anderson & Jansson, LLP
9501 N Capital of Texas Hwy #202
Austin, TX 78759
pehr@anjanlaw.com
512 372 8440 x200
512 233 2447 (fax)